# Towards post-quantum secure PAKE - A tight security proof for OCAKE in the BPR model

Nouri Alnahawi[1] *, Kathrin Hövelmanns[2], Andreas Hülsing[2] **, and Silvia Ritsch[2] ***

[1] Darmstadt University of Applied Sciences, Germany
[2] Eindhoven University of Technology, The Netherlands

**Abstract.** We revisit OCAKE (ACNS 23), a generic recipe that constructs password-based authenticated key exchange (PAKE) from key encapsulation mechanisms (KEMs), to allow instantiations with post-quantums KEM like KYBER.
The ACNS23 paper left as an open problem to argue security against quantum attackers, with its security proof being in the universal composability (UC) framework. This is common for PAKE, however, at the time of this submission's writing, it was not known how to prove (computational) UC security against quantum adversaries. Doing this becomes even more involved if the proof uses idealizations like random oracles or ideal ciphers.
To pave the way towards post-quantum security proofs, we therefore resort to a (still classical) game-based security proof in the BPR model (EUROCRYPT 2000). We consider this a crucial stepping stone towards a fully satisfying post-quantum security proof. We also hope that a game-based proof is easier to (potentially formally) verify.
We prove security of (a minor variation of) OCAKE, assuming the underlying KEM satisfies notions of ciphertext indistinguishability, anonymity, and (computational) public-key uniformity. Using multi-user variants of these properties, we achieve tight security bounds.
We provide a full detailed proof – something often omitted in publications on game-based security of PAKE. As a side-contribution, we demonstrate in detail how to handle password guesses, which is something we were unable to find in the existing literature at the time of writing.
Finally, we discuss which current PQC KEMs can be plugged into the proposed protocol and provide a concrete instantiation, accompanied by a proof-of-concept implementation and respective run-time benchmarks.

**Keywords:** Public-key cryptography, password-based authenticated key exchange, PAKE, CAKE, OCAKE, post-quantum cryptography, ROM, game-based security.

## 1 Introduction

A central problem of secure communication is how to securely agree on a shared secret key via public communication. The generic solution is called an authenticated key exchange (AKE) protocol, which usually uses public-key cryptography to agree on the shared secret. This is the basis of most modern secure communication protocols, including TLS, SSH, or WireGuard. The drawback of this solution is that it requires users to maintain a cryptographic key pair for authentication. As cryptographic keys are hard to memorize, they require secure storage with all the related challenges for usability. Hence, in many scenarios only the server is authenticated during the AKE protocol.

* N.A. was supported by National Research Center for Applied Cyber-Security ATHENE.

** A.H. was supported by an NWO VIDI grant (Project No. VI.Vidi.193.066).

*** S.R. is part of the Quantum-Safe Internet (QSI) ITN which received funding from the European Union's Horizon-Europe programme as Marie Sklodowska-Curie Action (PROJECT 101072637 - HORIZON - MSCA-2021-DN-01)